COMMITTEE PRINT

SHOWING THE TEXT OF H.R. 2577 AS FORWARDED BY THE SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE, JULY 20, 2011

112TH CONGRESS
1ST SESSION

H. R. 2577

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

IN THE HOUSE OF REPRESENTATIVES

JULY 18, 2011

Mrs. BONO MACK introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Secure and Fortify Electronic Data Act'' or the ''SAFE Data Act''.

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require any person engaged in interstate commerce that owns or possesses data containing personal information related to that commercial activity, including an information broker and any third party that has contracted with such person to maintain or process such data on behalf of such person, to establish and implement reasonable policies and procedures regarding information security practices for the treatment and protection of personal information, taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by, such person;

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(C) the cost of implementing such safeguards.

(2) DATA SECURITY REQUIREMENTS.—Such regulations shall, taking into consideration the quantity, type, nature, and sensitivity of the personal information, require the policies and procedures to include the following:

(A) A security policy with respect to the collection, use, sale, other dissemination, and maintenance of any data containing personal information.

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in each system maintained by such person that contains such data, which shall include regular monitoring to detect a breach of security of each such system.

(D) A process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and

to the architecture and installation of network or operating software.

(E) A process for disposing of data in electronic form containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

(b) DATA MINIMIZATION REQUIREMENTS.—A person subject to the requirements under subsection (a) shall establish a plan and procedures for minimizing the amount of personal information maintained by such person. Such plan and procedures shall provide for the retention of such personal information only as reasonably needed for the business purposes of such person or as necessary to comply with any legal obligation. The Commission may not promulgate any regulations with regard to the establishment of such plan and procedures.

(c) EXEMPTION FOR CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party

that is transmitted, routed, or stored in intermediate or transient storage by such service provider.

SEC. 3. NOTIFICATION AND OTHER REQUIREMENTS IN THE EVENT OF A BREACH OF SECURITY.

(a) REQUIREMENTS IN THE EVENT OF A BREACH OF SECURITY.—Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information related to that commercial activity, following the discovery of a breach of security of any system maintained by such person that contains such data, shall, without unreasonable delay—

(1) notify appropriate Federal law enforcement officials of the breach of security, unless such person determines that the breach involved no unlawful activity;

(2) take such steps necessary to prevent further breach or unauthorized disclosures;

(3) identify affected individuals whose personal information may have been acquired or accessed; and

(4) not later than 48 hours after identifying affected individuals under paragraph (3), unless the person makes a reasonable determination that the breach of security presents no reasonable risk of

identity theft, fraud, or other unlawful conduct affecting such individuals, notify—

(A) the Commission; and

(B) as promptly as possible, subject to subsection (c), each individual who is a citizen or resident of the United States whose personal information is known to have been acquired or accessed as a result of such a breach of security.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD PARTY AGENTS.—In the event of a breach of security of any third party entity that has contracted with a person to maintain or process data in electronic form containing personal information on behalf of such person, such third party entity shall—

(A) take the actions required under paragraphs (1) and (2) of subsection (a); and

(B) notify as promptly as possible such person of the breach of security.

Upon receiving notification from the third party entity under subparagraph (B), such person shall take the actions required under paragraphs (3) and (4) of subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another person engaged in interstate commerce that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data in connection with that commercial activity, such service provider shall—

(A) take the actions required under paragraphs (1) and (2) of subsection (a); and

(B) notify only the person who initiated such connection, transmission, routing, or storage, of the breach of security, if such person can be reasonably identified.

Upon receiving such notification from a service provider, such person shall take the action required under paragraphs (3) and (4) of subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a person is required to provide notification to more than 5,000 individuals under subsection (a)(4)(B), the person shall also notify the major credit reporting agencies that compile and maintain files on consumers on a

nationwide basis of the timing and distribution of the notices. Such notice shall be given to the credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMING AND DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(1) DEADLINE FOR COMMENCING NOTIFICATION.—Except as provided under paragraph (2) or (3), a person required to provide notification to individuals of a breach of security pursuant to subsection (a)(4)(B) shall begin to notify such individuals not later than 45 days after discovery of such breach.

(2) LAW ENFORCEMENT.—If a Federal law enforcement agency determines that the notification required under subsection (a)(4)(B) would impede a civil or criminal investigation, such notification shall be delayed upon the request of the law enforcement agency for 30 days or such lesser period of time that the law enforcement agency determines is reasonably necessary. The law enforcement agency shall follow up such a request in writing. A law enforcement

agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(3) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under subsection (a)(4)(B) would threaten national or homeland security, such notification may be delayed for a period of time that the national security agency or homeland security agency determines is reasonably necessary. The national security agency or homeland security agency shall follow up such a request in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(4)(B) shall be in compliance with such requirement if the person provides a conspicuous and clearly identified notifi-

cation by one of the following methods (provided the selected method can reasonably be expected to reach the intended individual):

(i) Written notification.

(ii) Notification by email or other electronic means, if—

(I) the person's primary method of communication with the individual is by email or such other electronic means; or

(II) the individual has consented to receive such notification and the notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A), such notification shall include—

(i) a description of the personal information that may have been acquired or accessed by an unauthorized person;

(ii) a telephone number that the individual may use, at no cost to such individual, to contact the person to inquire about the breach of security or the information the person maintained about that individual;

(iii) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions to the individual on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(iv) the toll-free contact telephone numbers and addresses for the major credit reporting agencies; and

(v) a toll-free telephone number and website address for the Commission whereby the individual may obtain information regarding identity theft.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(4)(B) may provide substitute notification in lieu of the direct notification required by paragraph (1) if the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals and such direct notification is not feasible due to—

(i) excessive cost to the person required to provide such notification relative to the resources of such person, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A); or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(4)(B);

(ii) a conspicuous notice on the website of the person (if such person maintains a website); and

(iii) notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired or accessed reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under this paragraph shall include—

(i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individuals, consumer credit re-

ports on a quarterly basis for a period of 2 years, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code; and

(ii) a telephone number by which an individual can, at no cost to such individual, learn whether that individual's personal information is included in the breach of security.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining circumstances under which substitute notification may be provided

under paragraph (2), including criteria for determining if notification under paragraph (1) is not feasible due to excessive costs to the person required to provide such notification relative to the resources of such person. Such regulations may also identify other circumstances where substitute notification would be appropriate for any person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this subsection. Such guidance shall include—

(i) a description of written or email notification that complies with the requirements of paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—A person required to provide notification under subsection (a)(4)(B) shall, in ac-

cordance with the determination described in paragraph (3), upon request of an individual whose personal information was included in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(A) consumer credit reports from at least one of the major credit reporting agencies beginning not later than 60 days following the individual's request and continuing on a quarterly basis for a period of 2 years thereafter; or

(B) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 60 days following the individual's request and continuing for a period of 2 years.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (d)(3), the Commission shall determine the circumstances under

which a person required to provide notification under subsection (a)(4)(B) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(f) PRESUMPTION CONCERNING DATA IN CERTAIN FORMS.—

(1) IN GENERAL.—If the data in electronic form containing personal information is unusable, unreadable, or indecipherable to an unauthorized person by encryption or other security technology or methodology (if the method of encryption or such other technology or methodology is generally accepted by experts in the information security field), there shall be a presumption, for purposes of subsection (a)(4), that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption or other security technologies or methodologies in a specific case have been or are reasonably likely to be compromised.

(2) METHODOLOGIES OR TECHNOLOGIES.—The Commission may issue guidance to identify security methodologies or technologies that render data in

electronic form unusable, unreadable, or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such methodology or technology in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

(g) WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(4)(A), finds that notification of such a breach of security available on the Commission's website would be in the public interest or for the protection of consumers, the Commission may place such a notice in a clear and conspicuous location on such website.

(h) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness

of requiring the notification required by subsection (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(i) GENERAL RULEMAKING AUTHORITY.—The Commission may promulgate regulations, pursuant to section 553 of title 5, United States Code, as necessary to effectively implement and enforce the requirements of this section.

SEC. 4. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 2 and 3 apply, according to their terms, to—

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding section 4 and section 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)), any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of such Code.

(b) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in viola-

tion of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates section 2 or 3 shall be subject to the penalties and entitled to the privileges and immunities provided in that Act, except that the Commission may not assess civil penalties for a violation of section 3(a)(1).

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates section 2 or 3 of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State

in a district court of the United States of appropriate jurisdiction—

(A) to enjoin further violation of such section by the defendant;

(B) to compel compliance with such section; or

(C) to obtain civil penalties in the amount determined under paragraph (2).

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 2.—For purposes of paragraph (1)(C) with regard to a violation of section 2, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a person is not in compliance with such section by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph (1)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than

$11,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is at least 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a person under this subsection, the maximum civil penalty for which any person may be liable under this subsection shall not exceed—

(i) $5,000,000 for all related violations of section 2; and

(ii) $5,000,000 for all violations of section 3 resulting from a single breach of security.

(3) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this

Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(d) ENTITIES GOVERNED BY HIPAA AND GRAMM-LEACH-BLILEY.—

(1) HIPAA.—

(A) INFORMATION SECURITY REQUIREMENTS.—To the extent that the information security requirements of part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.) apply in any circumstance to a person who is subject to such part, including as applied under subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.), such person shall be exempt from the requirements of section 2.

(B) NOTIFICATION REQUIREMENTS.—To the extent that the breach notification require-

ments of part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.) apply in any circumstance to a person who is subject to such part, including as applied under subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.), such person shall be exempt from the requirements of section 3.

(2) GRAMM-LEACH-BLILEY.—

(A) IN GENERAL.—Except as provided in subparagraph (B), a person who is subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.)—

(i) with regard to information security requirements, shall be exempt from the requirements of section 2; and

(ii) with regard to notification requirements, shall be exempt from the requirements of section 3.

(B) EXCEPTION.—Notwithstanding subparagraph (A), those persons subject to the jurisdiction of the Federal Trade Commission under section 505(a)(7) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)(7)) shall be subject to the requirements of this Act. If such

person is in compliance with the information security requirements of title V of such Act, such person shall be deemed in compliance with section 2 of this Act.

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) BREACH OF SECURITY.—The term ''breach of security'' means any unauthorized access to or acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(4) ENCRYPTION.—The term ''encryption'' means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management

and safeguards of such keys to protect the integrity of the encryption.

(5) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the name of such other person.

(6) INFORMATION BROKER.—The term ''information broker''—

(A) means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell such information or provide access to such information to any nonaffiliated third party in exchange for consideration, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity; and

(B) does not include a commercial entity to the extent that such entity processes information collected by or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or

former customers or employees of such third party to enable such third party directly or through parties acting on its behalf to provide benefits for its employees or directly transact business with its customers.

(7) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means an individual's first name or initial and last name, or address, or phone number, in combination with any 1 or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) PUBLIC RECORD INFORMATION.—Such term does not include public record information.

(C) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule, mod-

ify the definition of ''personal information'' under subparagraph (A)—

(i) for the purpose of section 2, to the extent that such modification is necessary to accomplish the purposes of such section as a result of changes in technology or practices and will not unreasonably impede technological innovation or otherwise adversely affect interstate commerce; and

(ii) for the purpose of section 3, if the Commission determines that access to or acquisition of the additional data elements in the event of a breach of security would create an unreasonable risk of identity theft, fraud, or other unlawful conduct and that such modification will not unreasonably impede technological innovation or otherwise adversely affect interstate commerce.

(8) PUBLIC RECORD INFORMATION.—The term ''public record information'' means information about an individual that is lawfully made available to the general public from Federal, State, or local government records.

(9) SERVICE PROVIDER.—The term ''service provider'' means a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such person transmits, routes, or stores, or for which such person provides connections. Any such person shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

SEC. 6. RELATION TO OTHER LAWS AND CONFORMING AMENDMENTS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to any entity subject to this Act, that contains—

(1) requirements for information security practices or treatment of data similar to those under section 2; or

(2) requirements for notification of a breach of security similar to the notification required under section 3.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 4(c) may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—This subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law.

(e) CONFORMING AMENDMENT.—Section 631(c)(1) of the Communications Act of 1934 (47 U.S.C. 551(c)(1))

is amended by striking ''and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator''.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 1 year after the date of enactment of this Act.